

ABSTRACT

An apparatus and method by which a user or cardholder can be given an Electronic-Commerce PIN that bears no discernible relation to the ATM PIN, but from which the ATM PIN can be cryptographically determined using the cardholder's account number and an issuer-unique "conversion" secret key. The intent is that the Maestro Master Debit Switch, or else the Member Interface Processor, whichever is appropriate to a given issuer, can "convert" an Electronic-Commerce PIN to an ATM PIN, so that the member, by verifying the ATM PIN, is in effect verifying the Electronic-Commerce PIN. If the Electronic-Commerce PIN is entered incorrectly, it will convert into an incorrect ATM PIN. Thus the member's EDP facility need not deal with two PINs, yet the ATM PIN is not exposed to possible compromise in PCs or other electronic-commerce equipment. The suggested approach ensures that any disclosure of the Electronic-Commerce PIN does not disclose the ATM PIN.